

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF SOUTH CAROLINA  
CHARLESTON DIVISION

UNITED STATES OF AMERICA,	)	CIVIL ACTION NO.: 2:25-cv-00672-DCN
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
305,845.298679 USDT,	)	
	)	
Defendant <i>in Rem</i> .	)	

**UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM***

The Plaintiff, United States of America, brings this complaint and alleges as follows.

**NATURE OF THE ACTION**

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 305,845.298679 Tether Crypto Currency (“USDT”) (“Defendant Funds”), pursuant to 18 U.S.C. § 981(a)(1)(C) and made applicable to criminal forfeiture by 28 U.S.C § 2461(c). The United States seeks forfeiture based upon reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes or is traceable to:

- a. Proceeds involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C § 1343 and/or conspiracy thereof;
- b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C § 1956;
- c. proceeds of cybercrimes or attempted cybercrimes in violation of 18 U.S.C § 1030.

**JURISDICTION AND VENUE**

2. This court has subject matter jurisdiction over an action commenced by the United States pursuant to 18 U.S.C § 981, and over an action for forfeiture virtue 28 U.S.C § 1355. This court has *in rem* jurisdiction over the Defendant Funds pursuant to:

- (a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and
- (b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

**THE DEFENDANT *IN REM***

3. The Defendant Funds consists of 305,845.298679 USDT valued at approximately \$304,454.31 In United States Currency, obtained by agents of the United States Secret Service (“USSS”) during an investigation into a transnational criminal organization, INC Ransomware Group, for running a malware fraud scheme. The funds were seized from a cryptocurrency decentralized wallet under the control of Tether LTD Associated, identified by account number (TC9...76Nch) and under the name of OKX User ID 421762047.

4. USSS agents seized the 305,845.298679 USDT, for federal forfeiture. The Defendant Funds are currently restrained and deposit to an account under the control of the United States Secret Service.

5. In accordance with the provisions of 19 U.S.C § 1606, the Defendant Funds have a total domestic value of approximately \$304,454.31 in United States Currency.

**KNOWN POTENTIAL CLAIMANTS**

6. The known entities and/or individuals whose interests may be affected by this litigation are:
- a. Account user: 421762047 (anaq19@mail.ru) who may have an interest in the Defendant Funds because they were the named account holder of the account seized by USSS during the investigation.

**BASIS FOR FORFEITURE**

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States based in part upon the following:

- a. USSS and local law enforcement agencies were investigating a transnational criminal organization running a malware fraud scheme. Investigating agents determined that a cybercrimes group had been targeting compromised IT networks to gain access to office software, files, and accounting systems of businesses to encrypt the files with an unknown malware variant. Once the cybercrimes group had encrypted the files, the group demanded a ransom payment be made to the decrypt the files. If the ransom payment was not paid by the victim, the decrypted files of the victim would be publicly posted on a TOR website. Payments made by victims were sent to a crypto currency wallet address provided by the suspects.

b. Cryptocurrency (also known as virtual currency or digital currency)<sup>1</sup> is a type of virtual currency, ad decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchange for fiat currency or other cryptocurrencies.<sup>2</sup> Examples of cryptocurrency are Bitcoin(BTC), Litecoin (LTC), Ethereum (ETH) and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.<sup>3</sup> Cryptocurrency is not illegal in the United States.

c. USDT is a digital stablecoin that is pegged to the United States dollar. USDT is managed by a consortium called Centre, which was founded by Circle and includes members from the cryptocurrency exchange Coinbase and Bitcoin mining company Bitmain, who are investors in Circle. Initially released in September 2018, the coin’s goal

---

<sup>1</sup> For the purposes of this complaint, the terms “digital currency,” “cryptocurrency,” and “virtual currency” are used interchangeably and address the same concept.

<sup>2</sup> Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

<sup>3</sup> Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

is to mirror the value of the United States dollar as a digital currency investment platform that matches the performance of the New York Stock Exchange as an alternative investment portfolio holding.

d. Tether (USDT) and Ethereum (ETH) is a type of cryptocurrency like Bitcoin (“BTC”).<sup>4</sup>

e. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long, and is somewhat analogous to a bank account number. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

f. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user

---

<sup>4</sup> Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

g. Although cryptocurrencies such as Bitcoin, Ethereum and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions

h. As of February 2, 2025, one USDT is worth approximately \$1.00 and one BTC is worth approximately \$96,620.41, though the value of USDT and BTC is generally much more volatile than that of fiat currencies. USDT value is directly tied to the value of the US Dollar and is traded on the ETH (ERC-20) or TRON (TRC-20) blockchain.

i. Cryptocurrency “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether/USDT. Exchanges can be brick-and-mortar businesses or online businesses (exchanging electronically transferred money and virtual currencies). According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.<sup>5</sup> Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers’ desire for anonymity, such exchangers are

---

<sup>5</sup> See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

j. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code with the public and private key embedded in the code.<sup>6</sup> Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their

---

<sup>6</sup> A QR code is a matrix barcode that is a machine-readable optical label.

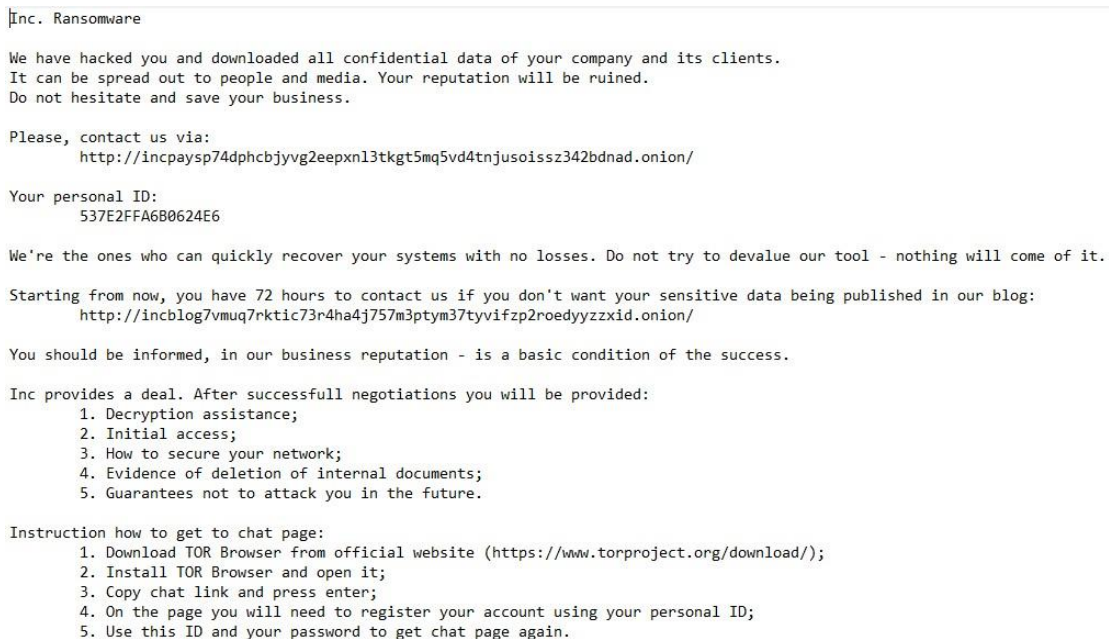


cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

k. OKX is a global cryptocurrency spot and derivatives exchange and the second biggest crypto exchange by trading volume, serving over 50 million people globally. Their registration shows Headquarters for this company is in the Republic of the Seychelles.

### **Use of Target Cryptocurrency Address to Defraud Victim 1**

8. On December 21, 2023, employees of the S.L. Firm (**Victim 1**), 15 Prioleau St, Charleston, SC 29401, found several pieces of paper printed out on their networked printers advising the firm that their business IT network had been compromised. Further investigation revealed that several endpoint workstations and servers have been compromised and encrypted using an unknown malware variant.



Inc. Ransomware

We have hacked you and downloaded all confidential data of your company and its clients. It can be spread out to people and media. Your reputation will be ruined. Do not hesitate and save your business.

Please, contact us via:  
<http://incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion/>

Your personal ID:  
537E2FFA6B0624E6

We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come of it.

Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:  
<http://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyzzxid.onion/>

You should be informed, in our business reputation - is a basic condition of the success.

Inc provides a deal. After successfull negotiations you will be provided:

1. Decryption assistance;
2. Initial access;
3. How to secure your network;
4. Evidence of deletion of internal documents;
5. Guarantees not to attack you in the future.

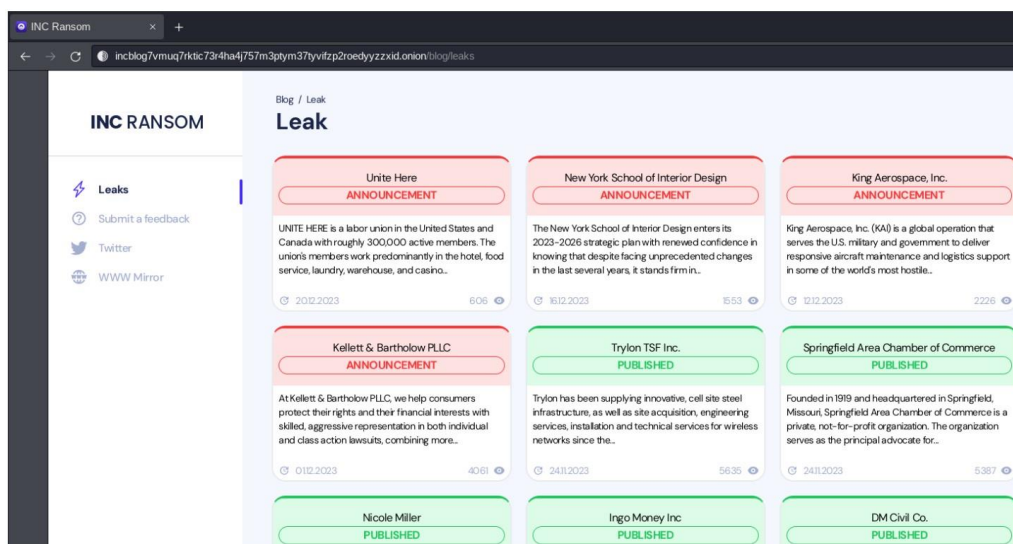
Instruction how to get to chat page:

1. Download TOR Browser from official website (<https://www.torproject.org/download/>);
2. Install TOR Browser and open it;
3. Copy chat link and press enter;
4. On the page you will need to register your account using your personal ID;
5. Use this ID and your password to get chat page again.

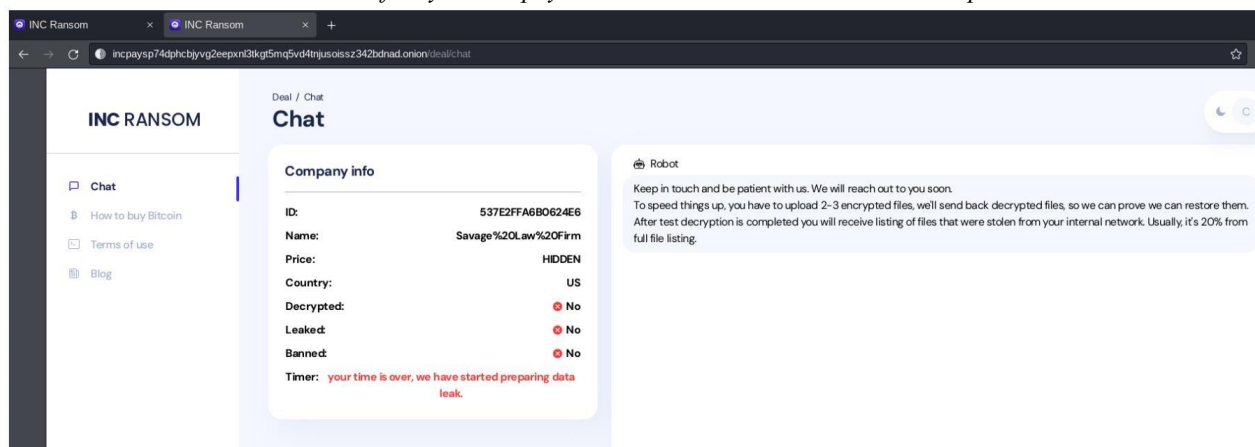
*Screenshot of printed ransomware note received by Victim 1 providing instructions how to use The Onion Router (TOR) and make the payment to INC Ransomware Group.*

9. On December 21, 2023, **Victim 1** filed iC3 report number I2312212202379381 to the Federal Bureau of Investigations (FBI) via computer crimes iC3 complaint website describing a ransomware attack on their business. The business computers and servers were encrypted, and all files were encrypted with the '.inc' file extension. As a result of the attack **Victim 1** was denied access to their office software, files, and accounting system.

10. On December 22, 2023, **Victim 1** retained a contract for cyber investigation and mitigation services with Infiltration Labs, LLC.

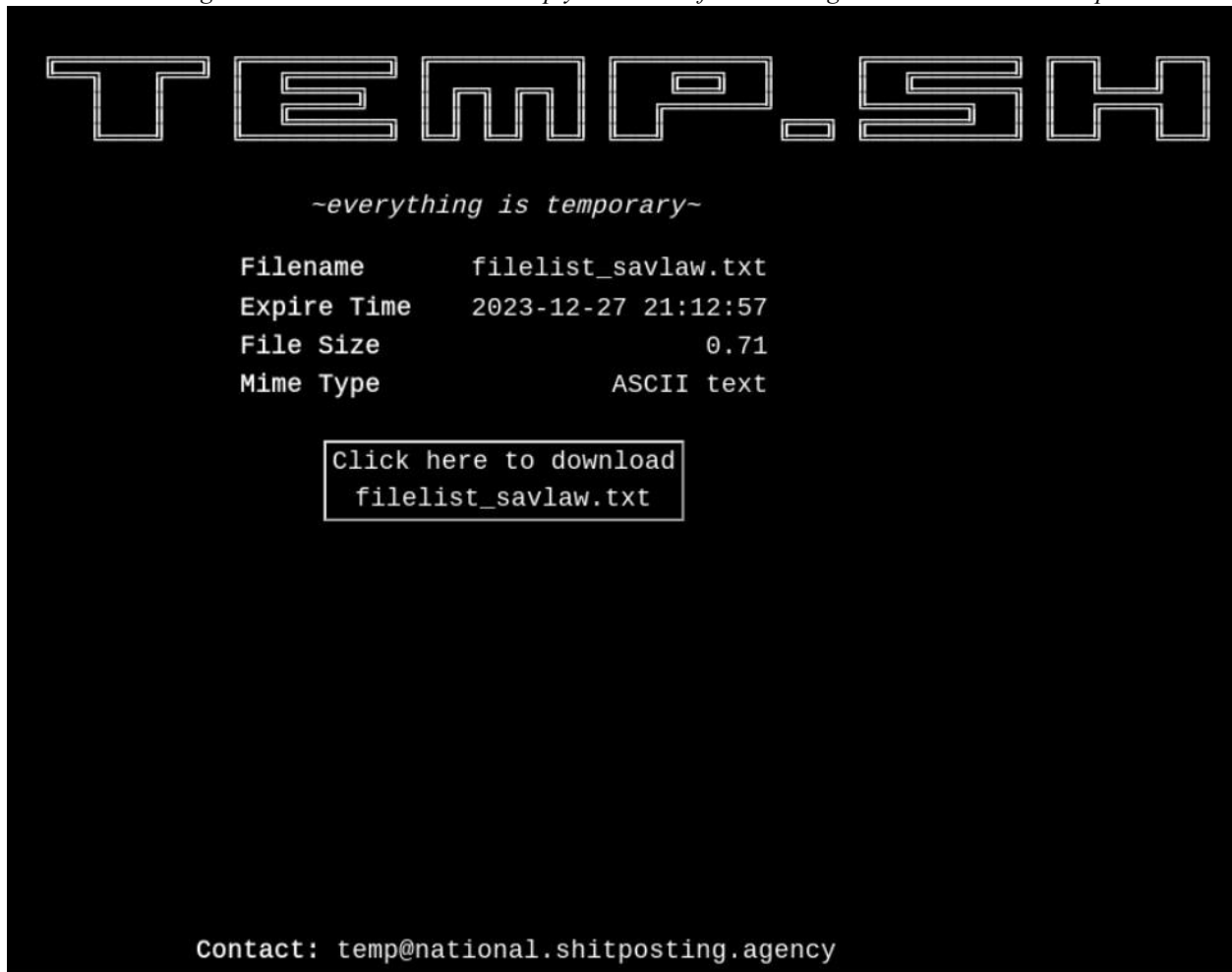


*Screenshot of the TOR site listed in the ransom note to see compromised hosts that Victim 1 will be added to if they do not pay the ransom taken on 12/22/23 at 3:28pm*



*Screenshot of the TOR site listed in the ransom note identifying the ID code which corresponds to S. L. Firm*

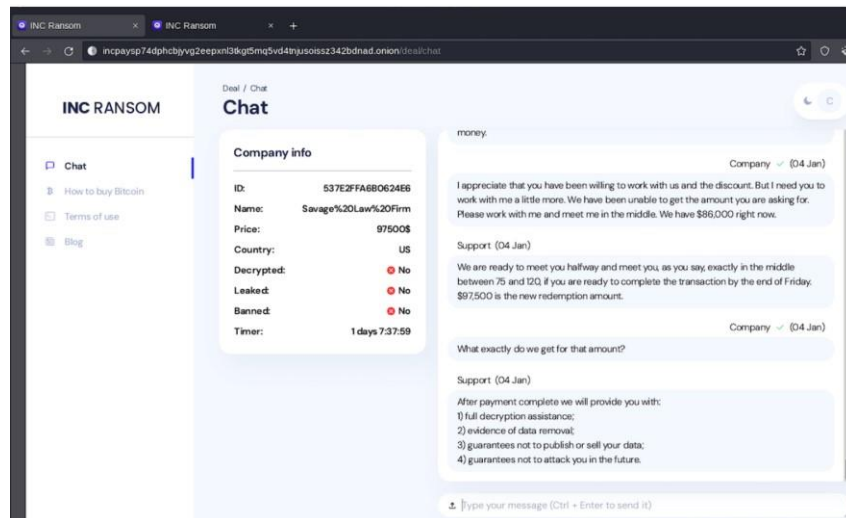
*as the target. Shows the automatic 'bot' reply in the chat feature. Image taken 12/22/23 at 3:52pm.*



*Screenshot showing the text file (filelist\_savlaw.txt) to be downloaded to show proof of stolen files. This screenshot also shows the contact email of the threat actor, temp@national.shitposting.agency. Image taken 12/24/23 at 8:33pm.*

11. On December 27, 2023, **Victim 1** filed a report with the Charleston Police Department, Case # 23-20513 and spoke with US Secret Service Task Force Officer James Jackson. **Victim 1** stated that IT systems were compromised sometime between 12/21/23 and 12/22/23 which included full system encryption and demanded a ransom payment be made to decrypt the files.

12. On January 4, 2024, final negotiations were made on the settlement price for the ransom payment through the TOR site and chat session. The original ransom was set at \$250,000.00, but subsequently negotiated down to \$97,500.00.



*Screenshot of final agreement chat log with threat actor showing the ransom amount to be paid.*

13. On January 9, 2024, **Victim 1** sent a wire transfer to Red Leaf Chicago, LLC d/b/a Digital Mint in the amount of \$105,925.00 for the purpose of payment to retrieve the decryption key for their files.

14. On January 10, 2024, email correspondence between mitigation company Infiltration Labs, LLC and Digital Mint show confirmation of payment to the threat actor (INC Ransomware Group).

From: Don Wyper <[dwyper@digitalmint.io](mailto:dwyper@digitalmint.io)>  
 Date: January 10, 2024 at 12:13:17 PM EST  
 Subject: Re: Ransomware Crypto Payment

Thank you. We are sending \$97,500 of bitcoin to bc1q7p83sex8h9uhfs5f3xqv29xrahluyvdwasysxj now

On Wed, Jan 10, 2024 at 12:09 PM Bryan Barnhart <[bryan@infiltrationlabs.com](mailto:bryan@infiltrationlabs.com)> wrote:

Ransomware Variant	INC
Ransomware note	Please see the attached screenshot. Original text or HTML can be provided on request
TA Wallet	bc1q7p83sex8h9uhfs5f3xqv29xrahluyvdwasysxj
Initial Demand	\$250,000
Final Demand	\$97,500
ETA	The deadline was yesterday (1/8/2024); however, we were granted an undetermined grace period.

I just reconfirmed the wallet with the TA.

Bryan Barnhart, GCFA, GPEN  
 Digital Forensics Incident Response Consultant  
 Infiltration Labs, LLC  
 954.779.6355  
[bryan@infiltrationlabs.com](mailto:bryan@infiltrationlabs.com)  
[www.infiltrationlabs.com](http://www.infiltrationlabs.com)

*Screenshot of email showing threat actor wallet address and amount paid by Don Wyper of Digital Mint to INC*

*Ransom Group via BTC wallet address bc1q7.....sysxj*

# 15. On January 10, 2024, Digital Mint paid the ransom on behalf of **Victim 1**

From: DigitalMint Cyber Settlement <[cyber@digitalmint.io](mailto:cyber@digitalmint.io)>  
 Date: January 10, 2024 at 7:05:08 PM EST  
 Subject: DigitalMint Cyber INVOICE 1-1632 - Project Savage Law

DIGITALMINT CYBER SETTLEMENT	INVOICE 1-1632
Project Name or Customer:	Project Savage Law
Transaction Date:	01/10/24
USD Amount Owed:	\$105,925.00
Transaction Amount:	2.12021000 BTC
Funding Status:	Wire Received - \$105,925.00
Transaction Details:	
Threat Actor (TA) Wallet	bc1q7p83sex8h9uhfs5f3xqv29xrahluyvdwasysxj
Transaction ID - TA Wallet	63f3bada747325971bd39ecce930da4db6e55d176e70eeaa66aa77590077c181
Client's LPOA Wallet	39Fao89MSXCuvWcQnfzGbSsz11izR8bkb
Transaction ID - LPOA Wallet	7cfe5f12ad11a35f01399f7234b4175add363a16467ff49631b011adb966d9a

Actions: No action, paid in advance  
 Invoice Due Date: Not applicable

DigitalMint Cyber Settlement  
[cyber@digitalmint.io](mailto:cyber@digitalmint.io)  
<https://cyber.digitalmint.io>

*Screenshot of Invoice 1-1632 provided by Digital Mint for payment services of INC Ransomware demand.*

16. On January 17, 2024, Infiltration Labs LLC provided the threat actor wallet address, transaction hash value, originating wallet address, type, and quantity of coin used to pay the ransom for further investigative leads to Network Intrusion Forensic Analyst (NIFA) Jonathan Van Houten of the Columbia Field Office Digital Forensic Laboratory.

17. On January 17, 2024, NIFA Van Houten provided the USSS the threat actor wallet address, transaction hash value, originating wallet address, type, and quantity of coin used to pay the ransom for digital currency forensics examination and tracing. Using WalletExplorer.com, the USSS followed the path of transactions from Victim 1 to the closest digital currency exchanger in an effort to identify the user of the threat actor wallet. The digital currency exchange identified with the money flow from Victim 1 was OKX.

18. On February 16, 2024, the USSS made an official request for information relating to the wallet address associated with OKX transactions for **Victim 1** ransom payment.



U.S. Department of Homeland Security  
UNITED STATES SECRET SERVICE

Date: 02/16/2024

OKX

RE: Request for Account Information and Ownership Verification

The United States Secret Service is requesting any account information that may assist the United States Secret Service in identifying the unknown account holder associated with OKX deposit addresses associate with TxID:

fbb171068751e506abb116221aa8fa24625393108d2eb3d8833b247cfba2e864

The compilation of records should include, but not be limited to the following: All records including customer name, photos, identifiers, telephone number(s), IP addresses and access logs, registration forms, transactional wallet and account records, email addresses, deposit records, opening documents, customer correspondence, and any other data that might assist in identifying the account holder or account activity. Records should also include any known methods of payment platforms to fund or liquidate such wallet.

IDENTIFIERS

Any and all accounts, API customer transactions, subscriber information or other OKX data related to any of the following identifiers, addresses, or wallets whom we have probable cause to believe are held at or directly interacting with OKX.

To OKX:

Any accounts that are the owners/operators/or controllers of the following transaction

Receiving address: 3Ky9yF6wXXWHi7TGYyzqYmiD1pgTUZ1Y22

Sending Address: bc1qpc0refm0g6fhht3hk7kjcwr2pdumcfcku3m4tv

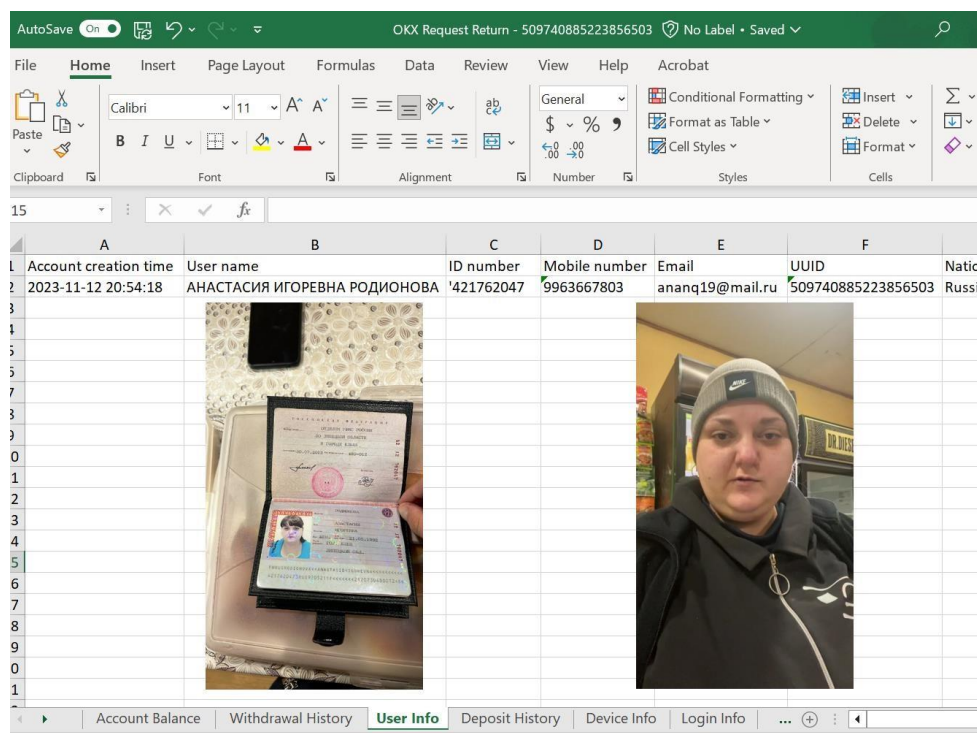
TXID: fbb171068751e506abb116221aa8fa24625393108d2eb3d8833b247cfba2e864

*Screenshot of requesting portion of the memo to OKX for transaction data regarding **Victim 1** ransom payment.*

19. On February 26, 2024, OKX returned the requested information via email in the format of an excel spreadsheet with multiple tabs containing valuable investigative leads such as User Information, Account balance, and Withdrawal History. These three tabs provided valuable insight on how the scheme was structured. User Information is also called Know Your Customer (KYC) data, which includes name, mobile device number, email address, and user photos for account opening purposes. Account balance data provided the USSS with an indication of the available funds and how the account has been used in the scheme, such as an exit node or money



laundering mechanism. The Withdrawal History provided the next step in continued forensic analysis of digital currency tracing to locate **Victim 1** funds.



*Screenshot of OKX Request Return data showing the User Info (KYC) data associated with **Victim 1** ransom payment.*

20. On March 4, 2024, additional tracing was conducted based on the withdrawal tab from the OKX return data. Confirmation tracing was conducted by Forensic Analyst (FA) with the US Secret Service Charlotte Field Office. This tracing effort confirmed funds being transferred from OKX account by user ID 421762047 to a decentralized wallet containing USDT (Tether). An official letter was sent to Tether for analysis of the ongoing investigation while requesting to freeze the wallet address and the contents therein as proceeds of Ransomware payments.





U.S. Department of Homeland Security  
**UNITED STATES SECRET SERVICE**

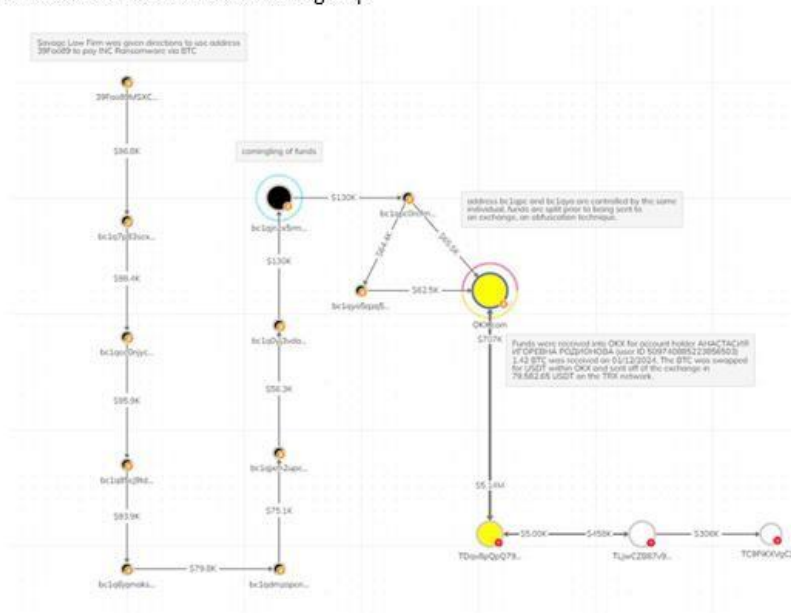
Columbia Field Office

107 Westpark Blvd Suite 301 Columbia, SC 29210

Tether Ltd  
inforequests@tether.to

Date: 03/04/2024

The tracing graph shown below depicts the flow of funds from our local victim to OKX, coin swapping from BTC to USDT and subsequently transferring to the address TC9PiKXVgCXPRbLeGmk1rng4hMuFx76Nch, which we assess is controlled by the same user or group of users associated with the INC ransomware group.



*Screenshot of the chart portion of the Tether Ltd request to freeze wallet address TC9...76Nch containing funds directly controlled by OKX User ID 421762047 which has direct involvement with **Victim 1** ransomware payment.*

21. On March 15, 2024, Tether provided an official response to the request and acknowledged the request by placing a freeze on the wallet address in question.

**From:** Tether Compliance <info@requests@tether.to>  
**Sent:** Friday, March 15, 2024 8:35 AM  
**To:** MATTHEW HANNON (CSC)  
**Subject:** Re: US Secret Service - Tether Freeze Request - Ransomware Victim Funds [#674231]

**Hello MATTHEW (CSC)**

Hello Agent Matthew Hannon,

We apologize for the delay in getting back to you.

We officially froze the address TC9PiKXVgCXPRbLeGmk1rng4hMuFx76Nch on March 8, 2024, which currently holds a balance of 305811 USDT. We kindly ask that you provide us with an official email address that we can use to refer third-party claimants (individuals claiming ownership of the wallet).

*Screenshot of Tether Ltd official response to the freeze request as proceeds of ransomware payment.*

22. It is common that criminal actors will shift the coin type and chain type to aid in funds obfuscation. This technique is referred to as chain hopping and coin swapping. In addition to chain hopping and coin swapping, here the bad actor hosted funds in a decentralized wallet.

23. On August 7, 2024, Tether contacted USSS about an individual claiming ownership of the Target Cryptocurrency Address. The person claimed to Tether that he or she believed the address was mistakenly identified as “dangerous” due to traffic from phishing scam addresses. Tether provided the person an official USSS email address to make this claim to the USSS. In the more than month that has passed, nobody has made a claim to the USSS email address provided.

24. On December 19, 2024, USSS received the Defendant 305,845.298679 USDT pursuant to a federal seizure warrant.

25. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. Proceeds of wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343 and/ or conspiracy to commit same;

b. Property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956;

c. Proceeds of cyber-crimes, in violation of 18 U.S.C. § 1030.

### CONCLUSION

26. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, in rem; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

ADAIR F. BOROUGHS  
UNITED STATES ATTORNEY

By: s/Carrie Fisher Sherard  
Carrie Fisher Sherard #10134  
Assistant United States Attorney  
55 Beattie Place, Suite 700  
Greenville, SC 29601  
(864) 282-2100

February 4, 2025